






SYSTEM FOR SENDING DOCUMENT AND METHOD THEREFOR

Publication number: JP11175607
Publication date: 1999-07-02
Inventor: HIROTA JUNKO; TAKEUCHI SATOSHI; YAMABE KOICHI
Applicant: HITACHI LTD
Classification:
 - international: **G06Q50/00; G06Q10/00; G06Q20/00; G07F17/16; G06Q50/00; G06Q10/00; G06Q20/00; G07F17/00; (IPC1-7): G06F17/60**
 - European: **G07F17/16**
Application number: JP19970352243 19971205
Priority number(s): JP19970352243 19971205

Also published as:

 E P0921484 (A2)
 US 6868402 (B1)
 E P0921484 (A3)
 CN16 04095 (A)
 CN14 97482 (A)

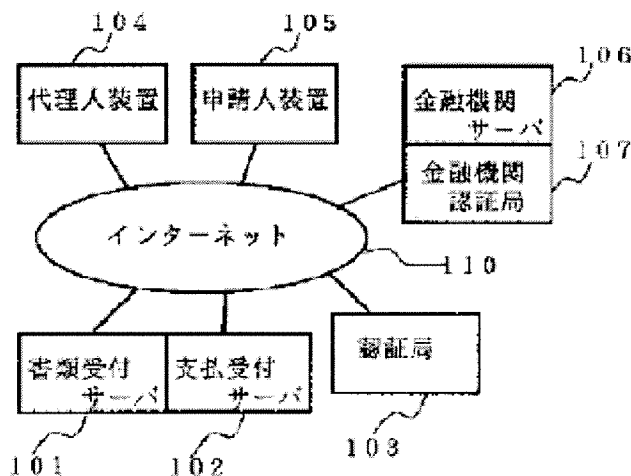
more >>

[Report a data error here](#)

Abstract of JP11175607

PROBLEM TO BE SOLVED: To properly attain electronic document sending and charge payment through communications without preparing any special account such as preliminary deposit account by connecting a payment accepting server with a network, and requesting charge payment to the payment accepting server by an applicant device.

SOLUTION: An applicant is connected from an applicant device 105 with a payment accepting server 102, and a charge payment processing is operated. The payment accepting server 102 is connected with a financial institution server 106, and the collation of the credit of the applicant is executed, and a payment certificate is transmitted to the applicant device 105. The applicant adds a payment certificate to document data, and transmits it to a substitute device 104. A substitute receives data by the substitute device 104, and temporarily preserves the data. In an arbitrary period, the substitute transmits the data to a document accepting server 101. The document accepting server 101 receives the data (data obtained by adding the payment certificate to the document data), verifies the payment certificate, and preserves the document data.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-175607

(43) 公開日 平成11年(1999) 7月2日

(51) Int.Cl.⁶

G 0 6 F 17/60

識別記号

F I

G 0 6 F 15/21

Z

審査請求 未請求 請求項の数 6 F D (全 20 頁)

(21) 出願番号

特願平9-352243

(22) 出願日

平成9年(1997)12月5日

(71) 出願人

000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者

廣田 純子

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者

武内 敏

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者

山部 浩一

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人

弁理士 矢島 保夫

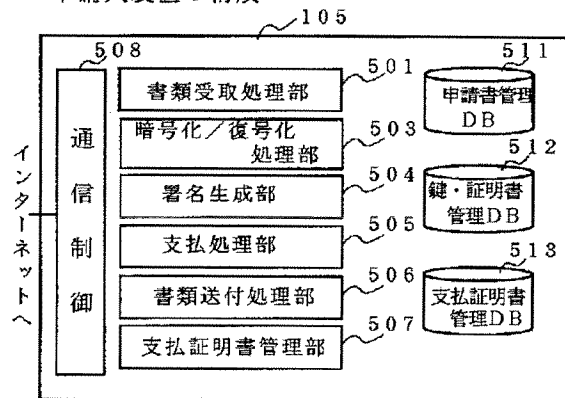
(54) 【発明の名称】 書類送付システムおよび方法

(57) 【要約】

【課題】 インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者が異なる場合でも適正に書類提出とその料金支払いを行なうことができる書類送付システムおよび方法を提供することを目的とする。また、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えた書類送付システムおよび方法を提供することを目的とする。

【解決手段】 ネットワーク上に支払い受付サーバを設け、該支払い受付サーバに対して支払い依頼を出せば、支払い受付サーバが信用照会を実施し、料金の支払いが保証される場合にはその旨を示す改ざん不可能な形式の支払い証明書を発行するようにする。書類を提出する際には、この支払い証明書を付して送信する。

申請人装置の構成



【特許請求の範囲】

【請求項1】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、

前記ネットワークに、支払い受付サーバを接続し、
前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、
前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を作成し、前記申請人装置に送信する手段とを備え、
前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信する手段を備え、
前記書類受付サーバは、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする書類送付システム。

【請求項2】ネットワーク経由で、申請人装置が送付したい書類を、代理人装置が代理して書類受付サーバに対して送付する書類送付システムにおいて、

前記ネットワークに、支払い受付サーバを接続し、
前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、
前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を作成し、前記申請人装置に送信する手段とを備え、
前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記代理人装置に送信する手段を備え、
前記代理人装置は、受信した支払い証明書付き書類を前記書類受付サーバに送信する手段を備え、
前記書類受付サーバは、前記代理人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする書類送付システム。

【請求項3】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、該書類の送付に伴う料金の支払いを受付ける支払い受付サーバであって、

前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、
該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を作成し、前記申

請人装置に送信する手段とを備えたことを特徴とする書類送付システムの支払い受付サーバ。

【請求項4】ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、

前記書類を送付する装置で、送付したい書類データに一方関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信する手段と、

10 前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信する手段と、

前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行する手段と、

前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認する手段とを備えたことを特徴とする書類送付システム。

20 【請求項5】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付方法において、

前記ネットワークに、支払い受付サーバを接続するとともに、

前記申請人装置から、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼するステップと、

30 前記支払い受付サーバにより、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施するステップと、

該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を作成し、前記申請人装置に送信するステップと、

前記申請人装置により、送付すべき書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信するステップと、

40 前記書類受付サーバにより、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管するステップとを備えたことを特徴とする書類送付方法。

【請求項6】ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付方法において、

前記書類を送付する装置で、送付したい書類データに一方関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信するステップと、

前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信するステップと、

前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行するステップと、

前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認するステップとを備えたことを特徴とする書類送付方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子データで各種の書類を送付・受付し、該書類の送付・受付に伴う料金の支払いやその支払い受付を行なう書類送付システムおよび方法に関する。

【0002】

【従来の技術】近年、インターネットのようなオープンなネットワーク環境において、各種の書類データの授受や商取引が行なわれるようになってきており、将来的にもさらに多種多様な形態になることが予測される。例えば、現在、特許庁への出願書類などの提出は、提出者が、直接、ダイヤルアップで特許庁のサーバに接続し提出書類データを送信することが可能になっているが、将来的にはインターネット経由で接続することが考えられる。一方、不動産登記や商業登記など、あるいは役所での住民票その他の証明書の発行業務などでは、申請する者が登記所や役所に直接出向いて書類（各種申請書）を提出して手続する必要があるが、このような業務も将来的にはインターネット経由で実施できるようになることが考えられる。

【0003】このようにインターネットなどを介して通信で電子的な書類提出を行なう場合、その書類提出に伴って手数料の支払いが必要になることがある。特許庁、登記所、あるいは役所などの官公庁に対して提出する書類では、印紙や証紙などを購入しそれを提出書類に貼付して提出する形態をとることが多いが、通信で書類提出を行なう場合には何らかの手数料支払いの仕組みが必要となる。特許庁の電子出願システムでは、あらかじめ書類提出者が予納口座に幾らかの金額を振込んでおき、特許庁の側のシステムでは出願を受け付けたときに当該予納口座から必要な金額を引き落とす形態を採る。

【0004】一方、いわゆる電子ショッピングなどと呼ばれる商取引では、インターネット経由で種々の商品を購入できるが、その支払いは、通常、クレジットカードや銀行口座からの引き落としで行なわれている。具体的には、商品を購入する者が、通信でクレジットカードや銀行口座の番号を送信し、商品を売る側ではその番号によってクレジットカードや銀行口座から所定の金額

を引き落とす。また、近年ではSET（Secure Electronic Transaction）と呼ばれるインターネットの電子決済方式なども提案されている。

【0005】

【発明が解決しようとする課題】上述したようにインターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合、特許庁の電子出願システムのような予納口座からの引き落としの方式では、書類提出を行なう者が必ず予納口座を作らなければならないと不便である。不動産登記などの申請では、その書類提出を行なう者が生涯に1度しかその手続を行なわないことも考えられるので、そのためだけに予納口座を作るのは面倒である。

【0006】予納口座によらない支払方法としては、クレジットカードや銀行口座からの引き落としがあるが、その場合は、申請者が指定したクレジットカードや銀行口座から引き落とす処理を、通信による書類の提出受け処理とは別フェーズで行なわなければならない。したがって、例えば口座に預金されている金額が引き落とし金額に満たないために引き落としができなくなるケースなどがある。

【0007】上述のSETのプロトコルによればインターネット上で電子決済できるが、これは商品を購入する者とその代金を支払う者が同じ者であって、商品購入の申込時に同時に決済を行なうことを前提としており、特許庁、登記所、あるいは役所などの官公庁に対して印紙や証紙などを貼付して書類を提出する形態の手続に適用するにはなじまない。そのような手続では、書類の申請者の代理人が申請者を代行して書類送付を行なう場合があるからである。すなわち、書類に添付する証紙や印紙などは書類の申請者が支払うべきものであり、一方、書類は代理人が提出するので、料金を支払う者と書類を提出する者とが異なることになり、その場合、書類の提出手続と関係付けつつSETのプロトコルで支払い手続を行なうことはできない。料金の支払いと書類の提出とを無関係に行なうのであれば、料金の支払いにSETのプロトコルを使用できるが、その場合は料金の支払い手続と書類の提出手続との関係付けがなされない。無理に関係付けようとすると、その分の手間がかかってしまう。

【0008】さらに、各種書類の提出に際して、その提出がいつ行なわれたかの日時を明確に確定することが必要な場合がある。一方、通信で書類提出を行なう場合は、通信回線の状態などに応じて再送が発生することがあり、書類の提出時点は明確でないという不都合がある。特に、書類の送信を開始した時点を書類の提出時点とした場合は、送信を開始して提出日時を確保した後、再送が発生したことを理由に後から別の内容の書類を送信し、その書類が前記提出日時に提出されたことと主張するような悪用が可能になってしまう。したがって、通信で書類を提出する際の提出時点を合理的に確定する仕組み

が求められている。

【0009】本発明は、上述の従来形における問題点を鑑み、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者が異なる場合でも適正に書類提出とその料金支払いを行なうことができる書類送付システムおよび方法を提供することを目的とする。

【0010】また、本発明は、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えた書類送付システムおよび方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するため、請求項1に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、前記ネットワークに、支払い受付サーバを接続し、前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信する手段を備え、前記書類受付サーバは、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする。

【0012】請求項2に係る発明は、ネットワーク経由で、申請人装置が送付したい書類を、代理人装置が代理して書類受付サーバに対して送付する書類送付システムにおいて、前記ネットワークに、支払い受付サーバを接続し、前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記代理人装置に送信する手段を備え、前記代理人装置は、受信した支払い証明書付き書類を前記書

類受付サーバに送信する手段を備え、前記書類受付サーバは、前記代理人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする。

【0013】請求項3に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、該書類の送付に伴う料金の支払いを受付ける支払い受付サーバであって、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備えたことを特徴とする。

【0014】請求項4に係る発明は、ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信する手段と、前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信する手段と、前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行する手段と、前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認する手段とを備えたことを特徴とする。

【0015】請求項5に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付方法において、前記ネットワークに、支払い受付サーバを接続するとともに、前記申請人装置から、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼するステップと、前記支払い受付サーバにより、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施するステップと、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信するステップと、前記申請人装置により、送付すべき書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信するステップと、前記書類受付サーバにより、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管するステップとを備えたことを特徴とする。

【0016】請求項6に係る発明は、ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付

10

20

30

40

50

する書類送付方法において、前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信するステップと、前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信するステップと、前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行するステップと、前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認するステップとを備えたことを特徴とする。

【0017】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態を説明する。

【0018】図1は、本発明の一つの実施の形態の書類送付システムの全体図である。インターネット110に、書類受付サーバ101、支払い受付サーバ102、認証局103、代理人装置104、申請人装置105、金融機関サーバ106、および金融機関認証局107が接続されている。

【0019】図1のシステムにおける処理の流れの概要を説明する。特に、暗号化/復号化処理やデジタル署名処理の説明は除き（それらについては後にフローチャートを参照して説明する）、データの流れに着目した処理の流れを説明する。

【0020】申請人装置105は、所定の料金を支払って書類を提出したい申請人が操作する装置であり、代理人装置104は、その申請人を代理して書類提出（実際の書類送信）を行なう申請人が操作する装置である。提出する書類は、まず申請人が、申請人の依頼に応じて代理人装置104で作成する。作成した書類データは、申請人装置105に送信する。申請人は、受信した書類データの内容を確認し、該書類データを保存しておく。また、申請人は、申請人装置105から支払い受付サーバ102に接続し、料金支払い処理を行なう。

【0021】支払い受付サーバ102は、書類提出に伴う料金の支払いに関する処理を行なうサーバであり、申請人装置105からの料金支払い処理要求を受けたときには、金融機関サーバ106に接続して当該申請人の信用照会を実施した後、支払い証明書を申請人装置105に返送する。支払い証明書は、申請人が料金支払いを行なったこと（あるいは、行なうことが保証されたこと）を証明するデータであり、印紙や証紙に相当するデータであるが、詳しくは後述する。支払い証明書は、書類受付サーバ101および支払い受付サーバ102の両者で共通にアクセス可能な支払い証明書管理データベース（DB）で管理される。申請人は、申請人装置105によりその支払い証明書を受信し、保存してあった書類デ

ータに支払い証明書を付けて代理人装置104に送信する。代理人は、代理人装置104により、該データを受信し、いったん保管する。その後任意の時期に、代理人は、該データを書類受付サーバ101に送信する。

【0022】書類受付サーバ101は、代理人装置104から送信されてくる提出書類を受付けるサーバである。書類受付サーバ101は、代理人から送信されたデータ（書類データに支払い証明書を付けたデータ）を受信し、支払い証明書を検証し書類データを保管する。支払い証明書の検証とは、当該支払い証明書が未使用のものであることを支払い証明書管理DBに問い合わせ、未使用であったら使用済みにする処理である。

【0023】認証局103は、申請人や代理人の認証を行なうために使用する証明書を発行する認証局である。金融機関サーバ106は、申請人の口座が設けられている金融機関のサーバである。金融機関認証局107は、その口座を持つ申請人の認証を行なうために使用する証明書を発行する認証局である。

【0024】図2は、図1の書類受付サーバ101および支払い受付サーバ102の内部構成を示す。

【0025】書類受付サーバ101は、チケット発行処理部211、書類受付処理部212、署名生成部213、暗号化/復号化処理部214、および通信制御部215を備えている。支払いサーバ102は、支払い受付処理部221、署名生成部222、暗号化/復号化処理部、支払い証明書生成管理部224、SET処理部225、および通信制御部226を備えている。また、書類受付サーバ101および支払いサーバ102の両方からアクセスできる共通データベース（DB）として、受付管理DB231、鍵・証明書管理DB232、申請人・代理人管理DB233、および支払い証明書管理DB234を備えている。

【0026】書類受付サーバ101は、インターネット110を介して代理人装置104から送信されてくる書類を受付ける。書類受付処理部212は、その書類受付処理（図18で詳しく説明する）を行なう。チケット発行処理部211は、書類受付処理を行なうにあたって、実際の書類データを受取る前にチケットを発行する処理（図17で詳しく説明する）を行なう。チケットの発行は、書類提出日時を決定するための処理である。すなわち、代理人装置104から書類受付サーバ101に書類を送付する際に、実際に送付しようとするデータをそのまま送信すると、再送が発生してその書類提出時点があまりになる恐れがあるので、以下の①～④のように処理して悪用を防ぐものである。

【0027】①まず代理人装置104で、実際に送付しようとするデータを一方向関数で圧縮しメッセージダイジェストを求め、該メッセージダイジェストを書類受付サーバ101に送る。（なお、詳しくは証明書付で暗号通信を行なう。）

②書類受付サーバ101では、チケット発行処理部211によるチケット発行処理(図17)で、新たな受付番号を取得し、該受付番号と該メッセージダイジェストを対応させて記憶するとともに、その受付番号を代理人装置104に送る。その受付番号を送るためのデータがチケットである。

③代理人装置104は、チケットにより受付番号を受取り、該受付番号を付けて実際に送付しようとするデータを、書類受付サーバ101に送る。

④書類受付サーバ101では、代理人装置104からのデータをすべて受信した後、そのデータを一方向関数(①で使用したのと同じ関数)で圧縮しメッセージダイジェストを求め、それが上記②で記憶してあるメッセージダイジェストと一致するか否かを確認する。一致すれば、チケット発行時に代理人装置104から実際に送付しようとしていたデータが実際に受信されたことになる。一方、一致しなければ、別のデータが送信されてきたことになる。

【0028】図8に、本実施の形態のシステムで書類受付サーバ101から代理人装置104に送られるチケットの内容を示す。受付番号801は、代理人装置104から書類送付する際に、その書類送付に対応して書類受付サーバ101が新たに割当てる番号である。送信者情報802は、その書類を送付する送信者(代理人)を特定する種々の情報である。有効期限803は、このチケットの有効期限を示す。代理人装置104から書類送付する際に、再送が発生しても当該書類の送付に十分な時間だけ有効期限(チケット発行時から所定時間を取ればよい)を取っておけばよい。無制限に遅れて書類送付されることを防ぐため、有効期限803を決めてある。署名804は、801~803のデータに対して書類受付サーバ101の署名を付したものである。

【0029】図9は、本実施の形態のシステムで使用する図1の受付管理DB231の内容を示す。書類受付サーバ101は、上記②のチケット発行処理(図17)で新たな受付番号を取得する際に、この受付管理DB231上で新たな受付番号を取得し、その受付番号に対応する1行分の領域を確保する。受付番号901、送信者情報902、および有効期限903には、送信したチケット(図8)に設定した情報801~803と同内容を記憶しておく。メッセージダイジェスト904、および送信者証明書905には、上記①で代理人装置104から送られてくる情報を記憶しておく。また、チケット管理情報906は、当該チケットが使用されたか否かのフラグ情報を記憶するもので、初期値は「未使用」にしておく。書類の内容907は、代理人装置104から送られてくる書類の全体を記憶しておく領域である。上記④でメッセージダイジェストの一致確認がなされたら、チケット管理情報906を「使用済み」とし、受信した書類データを書類の内容907に記憶するものである。

【0030】再び、図2に戻って、書類受付サーバ101の構成の説明を続ける。署名生成部213および暗号化/復号化処理部214は、書類受付処理を行なうにあたって、送受するデータに署名を付すとき、および暗号化/復号化処理を行なうときに使用する。通信制御部215は、インターネット110との間の通信制御を行なう。

【0031】支払い受付サーバ102は、申請人からの料金支払いを受付ける。この実施の形態のシステムでは、申請人は申請人装置105から支払い受付サーバ102に接続して、料金支払い処理を行なうことができる。支払い受付処理部221は、その申請人からの料金支払い要求を受付ける処理(図13で詳しく説明する)を行ない、申請人が料金支払いを行なったこと(あるいは支払うことが保証されたこと)を示す支払い証明書を申請人に発行する。支払い証明書は、印紙や証紙、あるいは金券や商品券のような役割を果たすものである。支払い証明書の発行は、当該申請人について金融機関に対して支払い信用照会を行なった上で発行するようになっているので、書類受け付けサーバ101および支払い受付サーバ102の運営機関は、支払い証明書を発行した金額については必ず当該申請人の口座から引き落としができる。また、支払い証明書は、予納とは異なり、あらかじめ予納口座を開く必要はない。支払い証明書は、印紙のように、別件に使用したり他人に贈与してもよい。

【0032】図6に、本実施の形態のシステムで用いる支払い証明書の内容を示す。支払い証明書は、管理番号601、支払い金額602、申請人情報603、有効期限604、および支払い受付サーバ102の署名605を備えている。管理番号601は、支払い証明書に固有の管理番号である。支払い金額602は、申請人が支払うことを指定した金額の情報である。申請人情報603は、支払い要求を出して当該支払い証明書を受け取った申請人を特定する情報である。有効期限604は、当該支払い証明書の有効期限である。署名605は、当該支払い証明書を発行した支払い受付サーバ102の署名であり、これにより当該支払い証明書が確かに支払い受付サーバ102から発行されたことが保証される。これらの情報601~605は、支払い受付サーバ102が当該支払い証明書を発行する際に設定するものである。

【0033】図7は、本実施の形態のシステムで使用する図1の支払い証明書管理DB234の内容を示す。支払い受付サーバ102は、発行した支払い証明書を、この支払い証明書管理DB234で管理する。支払い証明書管理DB234の701~705には、発行した支払い証明書の601~605の情報を記憶しておく。しよ状態706は、当該支払い証明書が使用されているか否かを示すフラグである。書類受付サーバ101が書類を受付けたとき、その書類に付いてきた支払い証明書の管理番号601で支払い証明書管理DB234を検索

し、対応するエントリを探す。そのエントリの使用状態706が「未使用」であれば、その支払い証明書は未だ使用されていないから、その使用状態706を「使用済み」とする。これは印紙や証紙などの貼付を確認することに相当するものである。再度同じ支払い証明書を使った書類が送付されてきたときは、使用状態706が「使用済み」であるので、料金支払いが保証されていないことが確認される。

【0034】図7のような支払い証明書管理DB234で支払い証明書を管理しているため、料金を支払う申請人と書類の送付を実際に実行する代理人とが異なる場合でも手続できる。また、支払い証明書を他人に譲渡して、その他人が使用することもできる。

【0035】再び、図1に戻って、支払い受付サーバ102の構成の説明を続ける。署名生成部222および暗号化/復号化処理部は、支払い受付処理を行なうにあたって、送受するデータに署名を付すとき、および暗号化/復号化処理を行なうときに使用する。支払い証明書生成管理部224は、図6の構成の支払い証明書を生成し、図7の支払い証明書管理DB234で管理する処理を行なう。SET処理部225は、支払い受付サーバ102から金融機関サーバ106に対して申請人の信用照会を行なう際にSETプロトコルにしたがう処理を行なう。通信制御部226は、インターネット110との間の通信制御を行なう。

【0036】書類受付サーバ101および支払いサーバ102の両方からアクセスできる共通DBである受付管理DB231および支払い証明書管理DB234については、図9および図7により説明した。鍵・証明書管理DB232は、この書類受付サーバ101および支払いサーバ102の秘密鍵、公開鍵、および認証局103、107から発行してもらった証明書、認証を行なう際に使用する認証局103、107の公開鍵、並びに、通信相手の公開鍵などを管理するDBである。申請人・代理人管理DB233は、この書類受付サーバ101および支払いサーバ102に接続してくる申請人や代理人に関する情報を管理するDBである。

【0037】なお、この実施の形態では、書類受付サーバ101と支払いサーバ102とを別装置で分け、共通DB203を共通に使用するような構成としたが、共通DBとせず、完全にDBを分けて構成してもよい。その場合は、受付管理DB231は書類受付サーバ101で管理し、支払い証明書管理DB234は支払い受付サーバ102で管理すればよい。逆に、書類受付サーバ101および支払いサーバ102をDB203も含めて1台の装置上に構成してもよい。その場合は、通信制御部、署名生成部、暗号化/復号化処理部などは共通の構成としてもよい。

【0038】図3は、図1の認証局103の構成を示す。認証局103は、証明書発行処理部301、証明書

管理部302、通信制御部304、および証明書管理DB311を備えている。認証局103は、あらかじめ代理人や申請人に証明書を発行する。

【0039】図4は、図1の代理人装置104の構成を示す。代理人装置104は、申請書エディタ401、署名生成部402、暗号化/復号化処理部403、書類送付処理部404、書類受取り処理部405、通信制御部406、申請書管理DB411、および鍵・証明書管理DB412を備えている。

【0040】申請書エディタ401は、送付する書類を作成するために使用するエディタである。書類送付処理部404は、申請人装置105に書類を送付する処理(図10で詳しく説明する)や、書類受付サーバ101に支払い証明書付き書類を送付する処理(図16で詳しく説明する)を行なう。書類受取り処理部405は、申請人から送られてくる支払い証明書付き書類の受取り処理(図15で詳しく説明する)を行なう。署名生成部402および暗号化/復号化処理部403は、送受するデータに署名を付すとき、および暗号化/復号化処理を行なうときに使用する。通信制御部406は、インターネット110との間の通信制御を行なう。

【0041】申請書管理DB411は、申請書エディタ401で作成した書類や、申請人から送られてくる支払い証明書付き書類を保存して管理するDBである。鍵・証明書管理DB412は、この代理人装置104の秘密鍵、公開鍵、および認証局103、107から発行してもらった証明書、認証を行なう際に使用する認証局103、107の公開鍵、並びに、通信相手の公開鍵などを管理するDBである。

【0042】図5は、図1の申請人装置105の構成を示す。申請人装置105は、書類受取り処理部501、受取り書類管理部502、暗号化/復号化処理部503、署名生成部504、支払い処理部505、書類送付処理部506、支払い証明書管理部507、通信制御部508、申請書管理DB511、鍵・証明書管理DB512、および支払い証明書管理DB513を備えている。

【0043】書類受取り処理部501は、代理人から送られてくる書類の受取り処理(図11で詳しく説明する)を行なう。支払い処理部505は、支払い受付サーバ102に接続して支払いを行なう処理(図12で詳しく説明する)を行なう。書類送付処理部506は、代理人に対して支払い証明書付き書類などを送付する処理(図14で詳しく説明する)を行なう。署名生成部504および暗号化/復号化処理部503は、送受するデータに署名を付すとき、および暗号化/復号化処理を行なうときに使用する。支払い証明書管理部507は、支払い受付サーバ102から発行してもらった支払い証明書を支払い証明書管理DB513で管理する処理を行なう。通信制御部508は、インターネット110との間

の通信制御を行なう。

【0044】申請書管理DB511は、代理人から送られてくる書類などを保存して管理するDBである。鍵・証明書管理DB512は、この申請人装置105の秘密鍵、公開鍵、および認証局103、107から発行してもらった証明書、認証を行なう際に使用する認証局103、107の公開鍵、並びに、通信相手の公開鍵などを管理するDBである。支払い証明書管理DB513は、支払い受付サーバ102から発行してもらった支払い証明書を保存して管理するDBである。その構成は、図7

で説明した支払い受付サーバ102の支払い証明書管理DB234と同じである。ただし、支払い証明書管理DB513は、この申請人が受け取った支払い証明書を管理するものであり、使用状態706はこの申請人が使用したか否かを示す情報である。

【0045】次に、図10～図18のフローチャートを参照して、図1のシステムにおける各処理の詳細を説明する。

【0046】図10は、代理人装置104から申請人装置105への書類送付の流れを示すフローチャートである。この処理は、主として図4の書類送付処理部404による処理である。まず代理人は、申請人の依頼に基づいて、図4の申請書エディタ401を用いて書類を作成しておく。ステップ1001で、送付する該書類に対して代理人の電子署名を実施する。具体的には、書類データを一方関数（ハッシュ関数など）で圧縮し、その圧縮データ（メッセージダイジェスト）を代理人の秘密鍵で暗号化した署名データを、元の書類データに付して、代理人署名付き書類を作る。次に、ステップ1002

で、代理人署名付き書類を暗号化する共通鍵を生成し、その共通鍵で代理人署名付き書類を暗号化する。次に、ステップ1003で、申請人の公開鍵によって前記共通鍵を暗号化する。ステップ1004では、暗号化された代理人署名付き書類と共通鍵を、代理人の証明書と共に申請人装置105に送信し、処理を終了する。

【0047】なお、代理人の証明書は、あらかじめ認証局103から取得しておく。代理人の証明書とは、代理人の公開鍵を該代理人に関する種々の情報と連結し、該連結データに対し認証局103の秘密鍵で署名を付したデータである。認証局103は、代理人から証明書発行依頼を受けたとき、当該代理人の身元確認を行なった後、証明書を発行する。代理人装置104から送信するデータにこの証明書を付ければ、当該データが確かに当該代理人から送られたものであることを、この証明書によって検証することができ、またこの証明書から代理人の公開鍵や代理人を特定する種々の情報を取得することができる。同様にして、申請人も、あらかじめ認証局103から証明書を取得しておく。

【0048】図11は、図10の処理により代理人装置104から申請人装置105へ送られたデータを受取る

申請人装置105の処理の流れを示す。この処理は、主として図5の書類受取り処理部501による処理である。まずステップ1101で、受信データ中の代理人の証明書を検証するとともに、受信データ中の暗号化された共通鍵を申請人の秘密鍵を用いて復号化する。ステップ1102で、復号化された共通鍵を用いて、代理人署名付き書類を復号化する。ステップ1103では、その代理人署名付き書類の署名を代理人の公開鍵を用いて検証する。この検証は、署名データを代理人の公開鍵で復号化した値が、書類データを一方関数（図10のステップ1001で使用したのと同じ関数を用いる）で圧縮した圧縮データ（メッセージダイジェスト）に等しくなるか否かを確認する処理である。検証の結果、適正な署名であったら、ステップ1105で当該代理人署名付き書類を保管する。検証の結果、適正な署名でなかったら、ステップ1106で申請書類が改ざんされていることを申請人に報告して、処理を終了する。

【0049】図12は、申請人による料金支払い処理の流れを示すフローチャートである。この処理は、主として図5の支払い処理部505による処理である。まずステップ1201で、申請人装置105から支払い受付サーバ102に接続し、支払い金額を決定・送信する。ステップ1202で、申請人の証明書（認証局103から取得した証明書）を支払い受付サーバ102に提示する。ステップ1203は、支払い受付サーバ102側の処理であり、図13で後述するが、支払い受付サーバ102からは、申請人の公開鍵で暗号化された共通鍵と該共通鍵で暗号化された支払い証明書（図6）が送信されてくる。ステップ1204では、支払い受付サーバ102から送信された暗号化された共通鍵を申請人の秘密鍵で復号化する。ステップ1205では、復号化された共通鍵を用いて、暗号化された支払い証明書を復号化する。ステップ1206で、復号化された支払い証明書を、支払い証明書管理DB513（図7）に保管して、処理を終了する。

【0050】図13は、図12のステップ1203の処理、すなわち支払い受付サーバ102における支払い受付処理の流れを示すフローチャートである。この処理は、主として図2の支払い受付処理部221による処理である。まず、ステップ1301で、申請人から送られた証明書を検証し、申請人の公開鍵を取得する。次にステップ1302で、例えばSETの Protokolを用いて、申請人からの支払い信用照会（与信）を金融機関に対して実施する。具体的には、図1の金融機関サーバ106に申請人と引き落とし金額を特定する情報を送信し、該申請人の口座からその引き落とし金額分を確保する。

【0051】なお、金融機関に対して支払い信用照会を実施する際、支払い受付サーバ102を運営する機関の身元を証明するため、あらかじめ支払い受付サーバ10

10

20

30

40

50

2を運営する機関は、金融機関認証局107から証明書を取得しておく必要がある。また、この支払い信用照会では、引き落としを行なう申請人についての認証も行なうので（確かにその申請人からの引き落とし依頼であるかどうかを確認する必要がある）、あらかじめ申請人は金融機関認証局107から証明書を取得しておくとともに、その金融機関の証明書をステップ1202で支払い受付サーバ102に送り、支払い受付サーバ102はステップ1302で信用照会するときその申請人の金融機関の証明書を付けて信用照会する必要がある。

【0052】ステップ1302の信用照会の結果、ステップ1303で、上記引き落とし金額分の引き落とし枠が確保できたらステップ1304に進む。信用照会結果に何らかの問題があったら、処理を終了する。ステップ1304では、新たに発行する支払い証明書の管理番号を取得する。具体的には、図7の構成の支払い証明書管理DB234で新規管理番号の一行分の領域を確保する。次に、ステップ1305で、申請人の証明書から申請人を特定する情報を抽出する。ステップ1306では、管理番号、支払い金額、申請人を特定する情報、および有効期限を連結したデータに電子署名を実施して、支払い証明書（図6）を作成する。具体的には、上記連結データを一方向関数（ハッシュ関数など）で圧縮し、その圧縮データを支払い受付サーバ102の秘密鍵で暗号化した署名データを、元の連結データに付して、支払い証明書を作る。

【0053】ステップ1307では、作成した支払い証明書に含めた情報を支払い証明書管理DB234（図7）に記録する。そして、ステップ1308で、支払い証明書を暗号化するための共通鍵を生成し、その共通鍵で支払い証明書を暗号化する。次に、ステップ1309で、申請人の公開鍵によって前記共通鍵を暗号化する。ステップ1310では、暗号化された共通鍵と該共通鍵で暗号化された支払い証明書とを申請人装置105に送信し、処理を終了する。

【0054】図14は、申請人装置105から代理人装置104への書類送付の流れを示すフローチャートである。この処理は、主として図5の書類送付処理部506による処理である。まずステップ1401で、図11のステップ1105で保管してある代理人署名付き書類を取り出す。ステップ1402では、代理人署名付き書類と支払い証明書とを含めたデータに対して、申請人の電子署名を実施する。これを支払い証明書付き書類と呼ぶ。なお、ここで使用する支払い証明書は、図7の構成の支払い証明書管理DB513で管理されている支払い証明書のうち、使用状況706が「未使用」のものを使用する。使用した支払明細書の使用状況706は「使用済み」に変更しておく。

【0055】次に、ステップ1403で、共通鍵を生成し、該共通鍵で支払い証明書付き書類を暗号化する。ス

テップ1404で、代理人の公開鍵を用いて、前記共通鍵を暗号化する。ステップ1405では、暗号化された共通鍵と該共通鍵で暗号化された支払い証明書付き書類を代理人装置104に送信する。

【0056】図15は、図14で送信された申請人からのデータを受取る代理人装置104の処理の流れを示すフローチャートである。この処理は、主として図4の書類受取り処理部405による処理である。まずステップ1501で、受信データ中の暗号化された共通鍵を代理人の秘密鍵を用いて復号化する。ステップ1502で、復号化された共通鍵を用いて、支払い証明書付き書類を復号化する。ステップ1503では、その支払い証明書付き書類に添付されている申請人の電子署名を申請人の公開鍵を用いて検証する。この検証は、署名データを申請人の公開鍵で復号化した値が、支払い証明書付き書類を一方関数（図14のステップ1402の署名で使ったのと同じ関数）で圧縮した圧縮データに等しくなるか否かを確認する処理である。

【0057】ステップ1504で、検証の結果、適正な署名であったら、ステップ1506に進む。ステップ1506では、支払い証明書付き書類に含まれている支払い証明書の電子署名を支払い受付サーバ102の公開鍵を用いて検証する。この検証は、署名データを支払い受付サーバ102の公開鍵で復号化した値が、支払い証明書に含まれている管理番号、支払い金額、申請人を特定する情報、および有効期限を連結したデータを一方関数（図13のステップ1306の署名で使ったのと同じ関数）で圧縮した圧縮データに等しくなるか否かを確認する処理である。

【0058】ステップ1507で、検証の結果、適正な署名であったら、ステップ1509に進む。ステップ1509では、支払い証明書付き書類に含まれている代理人署名付き書類中の代理人の署名を、代理人の秘密鍵を用いて検証する。ステップ1510で検証結果が適正な署名であったら、ステップ1512で支払い証明書付き書類を保管して、処理を終了する。ステップ1504、1507、1510の何れかのステップで、検証結果が不正な署名であることを示していたら、それぞれ、ステップ1505、1508、1511で書類が改ざんされていることを代理人に報告して、処理を終了する。

【0059】図16は、代理人装置104から書類受付サーバ101への支払い証明書付き書類の送付処理の流れを示すフローチャートである。この処理は、主として図4の書類送付処理部404による処理である。まずステップ1601で、送付しようとする支払い証明書付き書類を一方関数で圧縮し、圧縮データ（メッセージダイジェスト）を生成する。次に、ステップ1602で、共通鍵を生成し、該共通鍵で上記メッセージダイジェストを暗号化する。ステップ1603では、上記共通鍵を書類受付サーバ101の公開鍵で暗号化する。ステップ

1604では、暗号化された共通鍵と該共通鍵で暗号化されたメッセージダイジェストに、代理人の証明書を添付して書類受付サーバ101に送付する。ステップ1605は、書類受付サーバ101側のチケット発行処理であり、図17で後述するが、書類受付サーバ101からは、代理人の公開鍵で暗号化された共通鍵（書類受付サーバ101側で生成した鍵）と該共通鍵で暗号化されたチケット（図8）が送信されてくる。

【0060】ステップ1606では、書類受付サーバ101から送られてきた暗号化された共通鍵を、代理人の秘密鍵を用いて復号化する。ステップ1607では、復号化された共通鍵を用いてチケットを復号化する。次に、ステップ1608で、書類受付サーバ101の公開鍵を用いて、チケット（図8）に付いている電子署名を検証する。ステップ1609で、検証結果が適正な署名であることを示していたら、書類受付サーバ101が提出日時を確保したということであるから、ステップ1611に進む。ステップ1609で、不正な署名であったら、ステップ1610でチケットが改ざんされていることを代理人に報告し、処理を終了する。

【0061】チケットが取れたら、ステップ1611で共通鍵を生成し、ステップ1612で支払い証明書付き書類を該共通鍵で暗号化する。ステップ1613では、該共通鍵でチケットを暗号化する。次に、ステップ1614で、書類受付サーバ101の公開鍵で上記共通鍵を暗号化する。そして、ステップ1615で、暗号化した共通鍵、および該共通鍵で暗号化したチケットと支払い証明書付き書類を書類受付サーバ101に送付する。ステップ1616は、書類受付サーバ101側の処理であり、図18で後述するが、書類受付サーバ101からは、代理人の公開鍵で暗号化された共通鍵と該共通鍵で暗号化された受付確認書が送信されてくる。

【0062】ステップ1617では、書類受付サーバ101から送信された暗号化された共通鍵を代理人の秘密鍵で復号化する。ステップ1618では、復号化された共通鍵を用いて、暗号化された受付確認書を復号化する。ステップ1619で、受付確認書に添付された書類受付サーバ101の電子署名を検証する。ステップ1620で検証結果が適正な署名であることを示していたら、ステップ1622で、受付確認書を保管して、処理を終了する。ステップ1620で、検証結果が不正な署名であることを示していたら、ステップ1620で何らかのデータ改ざんがなされたことを代理人に報告し、処理を終了する。

【0063】図17は、図16のステップ1605の処理、すなわち書類受付サーバ101のチケット発行処理の流れを示すフローチャートである。この処理は、主として図2のチケット発行処理部211による処理である。まずステップ1701で、書類受付サーバ101の秘密鍵を用いて、代理人から送られてきた共通鍵を復号

化する。次に、ステップ1702で、該共通鍵を用いてメッセージダイジェストを復号化する。そして、ステップ1703で、新たな受付番号を取得し、該受付番号901、代理人（送信者）に関する情報902、有効期限903、メッセージダイジェスト904、および代理人の証明書905を、受付管理DB231（図9）に保管する。なお、代理人に関する情報は、代理人から送られてきたデータに含まれている代理人の証明書から抽出した情報を設定する。有効期限は、現時点に所定時間を加えた時間を設定する。また、チケットの管理情報906は「未使用」に初期化しておく。

【0064】次に、ステップ1704では、受付番号と、代理人に関する情報と、有効期限とを連結したデータを生成し、該連結データに対して電子署名を実施する。この電子署名付きデータがチケット（図8）である。具体的には、上記連結データを一方向関数（図16のステップ1601や1608で用いたのと同じ関数）で圧縮し、その圧縮データを書類受付サーバ101の秘密鍵で暗号化した署名データを、元の連結データに付して、チケット（図8）を作る。次に、ステップ1705で、共通鍵を生成し、該共通鍵で上記チケットを暗号化する。ステップ1706では、代理人の公開鍵を用いて、上記共通鍵を暗号化する。ステップ1707で、暗号化された共通鍵、および該共通鍵で暗号化されたチケットを代理人に対して送付し、処理を終了する。

【0065】図18は、図16のステップ1616の処理、すなわち書類受付サーバ101による書類受付処理の流れを示すフローチャートである。この処理は、主として図2の書類受付処理部212により実行される処理である。まずステップ1801で、書類受付サーバ101の秘密鍵を用いて、代理人から送られてきた共通鍵を復号化する。ステップ1802で、復号化された共通鍵を用いて、チケットと支払い証明書付き書類を復号化する。次に、ステップ1803で、チケットに付いている電子署名、および有効期限を検証する。検証の結果、ステップ1804で、署名も適正で有効期限内であるときは、ステップ1806に進む。署名が不正、または有効期限が過ぎていた場合は、ステップ1805でチケット不正を表示して、処理を終了する。

【0066】ステップ1806では、代理人から送付されてきた支払い証明書付き書類を、代理人装置104で使用した一方向関数（図16のステップ1601や1608で用いたのと同じ関数）で圧縮し、メッセージダイジェストを生成する。ステップ1807では、代理人から送付されてきたチケットから受付番号を取り出し、受付管理DB231（図9）を参照して、当該受付番号に対応するチケット請求時のメッセージダイジェストを取り出し、ステップ1806で生成したメッセージダイジェストと比較する。比較の結果、ステップ1808で同一であれば、確かにチケット請求時に送ろうとしてい

た内容が送られてきたものと認められるので、ステップ1810に進む。ステップ1808で比較の結果が同一でないときは、チケット請求時に送ろうとしていた内容と別の内容が送られてきたということだから、ステップ1809で送付データ不一致の表示を行ない、処理を終了する。

【0067】ステップ1810では、支払い証明書に含まれている管理番号のデータを支払い証明書管理DB234(図7)から検索し、その使用状況706が「未使用」であるか否かを検証する。ステップ1811で、

「未使用」であったときは、ステップ1813で、支払い証明書管理DB234の当該管理番号の支払い証明書の使用状況706を「使用済み」に変更する。次に、ステップ1814で、当該受付番号のチケットの管理情報906を「使用済み」に変更する。そして、ステップ1815で、支払い証明書付き書類を保管する。書類の保管は、図9の受付管理DB231の書類の内容907に格納することにより行なう。

【0068】さらに、ステップ1816で、受付番号などの受付情報を含む受付確認書を作成し、電子署名を実行する。ステップ1817で、共通鍵を生成し、該共通鍵で上記電子署名付き受付確認書を暗号化する。ステップ1818では、代理人の公開鍵で上記共通鍵を暗号化する。ステップ1819で、暗号化した共通鍵、および該共通鍵で暗号化した電子署名付き受付確認書を代理人に送付して、処理を終了する。

【0069】上記実施の形態のシステムによれば、申請人が支払い証明書を取得し、代理人が提出書類に支払い証明書を付けて、書類受付サーバに送付することが可能になる。支払い証明書は、印紙や証紙、金券や商品券のようなイメージで使用することができ、支払い受付サーバの署名が付いているので容易に改ざんされない。実際の決済はどのような形態で行なってもよいが、与信の段階で引き落とし可能であることが保証されるので、書類受付サーバの側では必ず料金を徴収できる。また、申請人が書類に支払い証明書を付けて、その全体に署名を付して、代理人に送っているのだから、申請人が当該書類の内容で了解しているという意志表示をしたことになるし、その後代理人が書類を改ざんすることもできない。

【0070】さらに、書類提出時点を決定する際、始めに提出者から送付しようとする書類データを一方向関数で圧縮してメッセージダイジェストを求め、これを証明書と一緒に書類受付サーバに送り、書類受付サーバではそのメッセージダイジェストを記憶して、チケットを返す。その後、提出者から書類データの全体が送られてきたときには、そのメッセージダイジェストを求めて、チケット発行時に記憶してあるメッセージダイジェストと比較することで、当初から送る予定の書類が確かに送られてきたことを確認できる。そのため、チケット発行時を書類提出時点とみなすことができるようになる。

【0071】なお、上記実施の形態では、代理人が申請者を代理して書類提出を行なう例を説明したが、代理人経由でなく、直接、申請人が書類受付サーバに対する書類送付を行なうようにしてもよい。

【0072】また、上記実施の形態では、支払方式としてSETを用いた例を説明したが、SET以外の支払方式、例えばSETを使わないクレジットカード支払いの方式などを用いてもよい。

【0073】本発明は、特許庁、登記所、あるいは役所などの官公庁に対してインターネット経由で書類を送付する場合などに適用可能である。また、いわゆる電子ショッピングなどに適用することも可能である。

【0074】

【発明の効果】以上説明したように、本発明によれば、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、支払い受付サーバに対して支払い依頼を出せば、支払い受付サーバが信用照会を実施し、料金の支払いが保証される場合にはその旨を示す改ざん不可能な形式の支払い証明書を発行してくれるので、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なう場合に引き落とせないというようなことも無く、また料金を支払う者と書類の提出を行なう者とが異なる場合でも適正に書類提出とその料金支払いを行なうことができる。

【0075】また、書類を送付する前に、送付する書類を一方向関数で圧縮した圧縮データを送り、あとで実際に送られてきた書類に対して同じ一方向関数で圧縮した圧縮データと比較確認しているのだから、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みが提供される。

【図面の簡単な説明】

【図1】本発明の実施の形態の書類送付システムの全体図

【図2】書類受付サーバおよび支払い受付サーバの内部構成図

【図3】認証局の構成図

【図4】代理人装置の構成図

【図5】申請人装置の構成図

【図6】本実施の形態のシステムで用いる支払い証明書の内容を示す図

【図7】本実施の形態のシステムで使用する支払い証明書管理DBの内容を示す図

【図8】本実施の形態のシステムで書類受付サーバから代理人装置に送られるチケットの内容を示す図

【図9】本実施の形態のシステムで使用する受付管理DBの内容を示す図

【図10】代理人装置から申請人装置への書類送付の流れを示すフローチャート図

【図11】代理人装置から申請人装置へ送られたデータ

を受取る申請人装置の処理の流れを示すフローチャート図

【図12】申請人による料金支払い処理の流れを示すフローチャート図

【図13】支払い受付サーバにおける支払い受付処理の流れを示すフローチャート図

【図14】申請人装置から代理人装置への書類送付の流れを示すフローチャート図

【図15】申請人からのデータを受取る代理人装置の処理の流れを示すフローチャート図

【図16】代理人装置から書類受付サーバへの支払い証*

*明書付き書類の送付処理の流れを示すフローチャート図

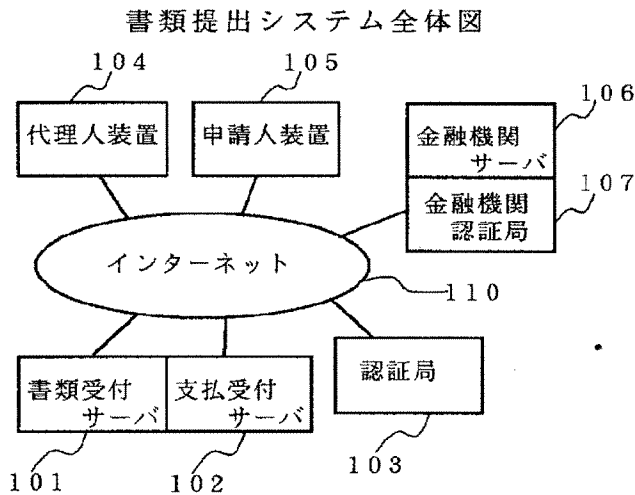
【図17】書類受付サーバのチケット発行処理の流れを示すフローチャート図

【図18】書類受付サーバによる書類受付処理の流れを示すフローチャート図

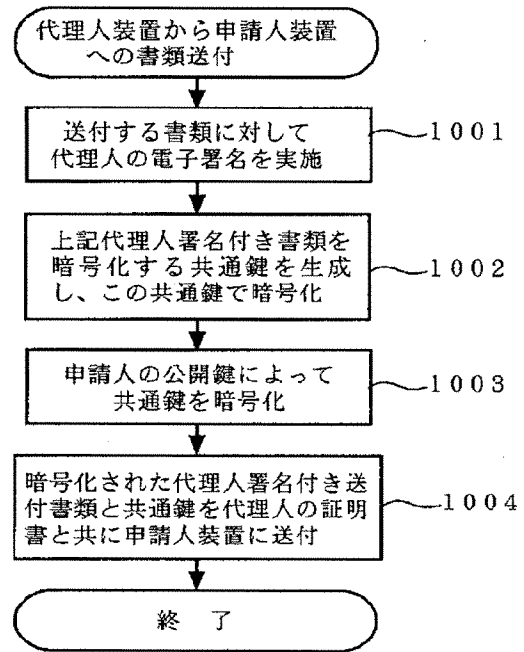
【符号の説明】

101…書類受付サーバ、102…支払い受付サーバ、103…認証局、104…代理人装置、105…申請人装置、106…金融機関サーバ、107…金融機関認証局、110…インターネット。

【図1】

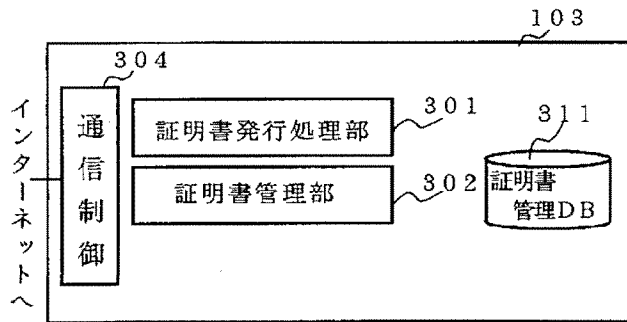


【図10】

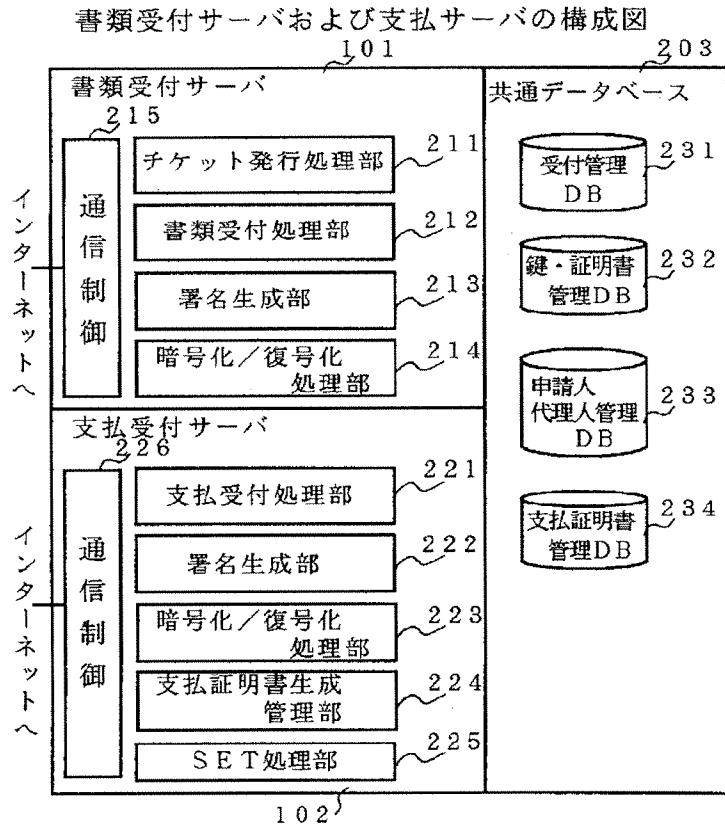


【図3】

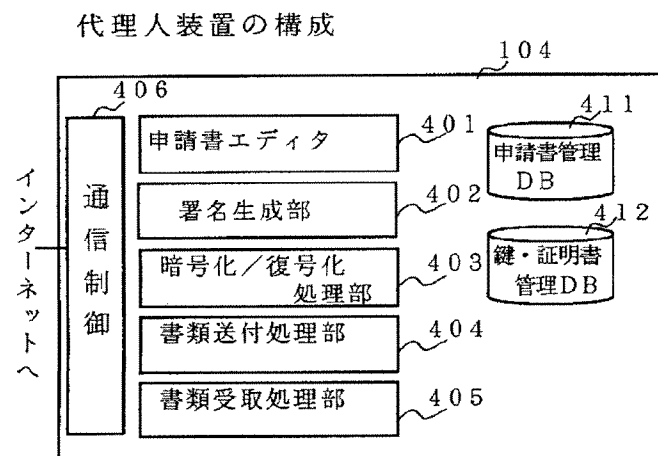
認証局の構成



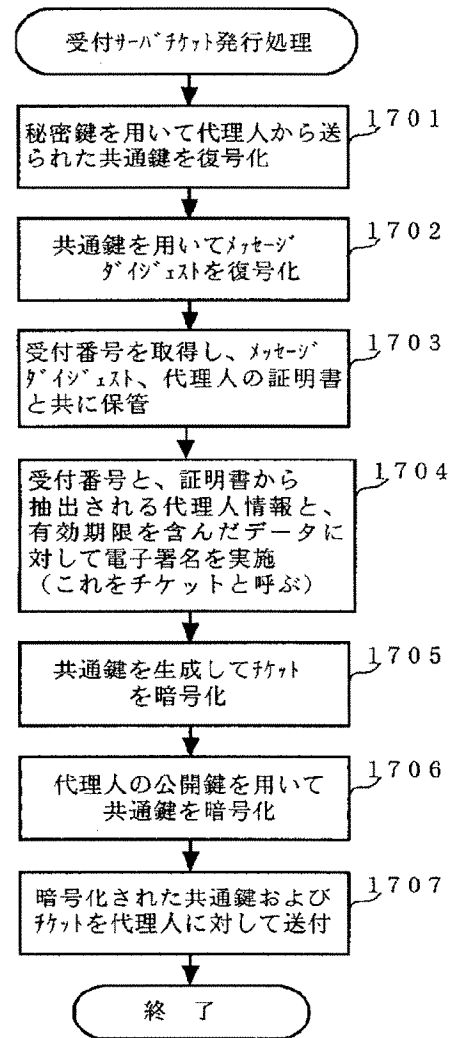
【図2】



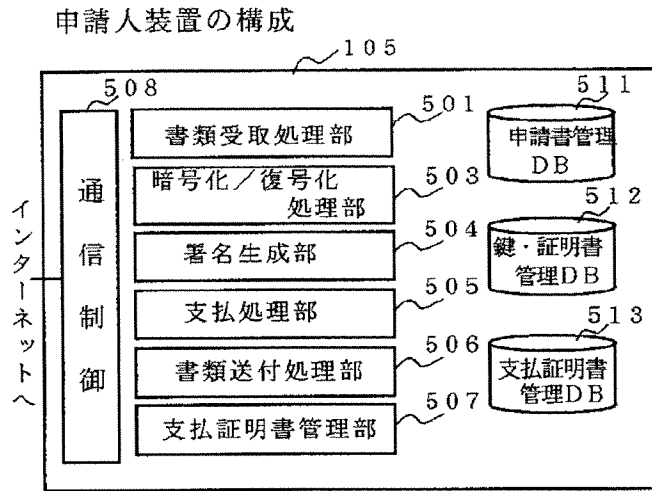
【図4】



【図17】



【図5】



【図6】

支払証明書の内容

| | | | | |
|------|------|-------|------|-----|
| 601 | 602 | 603 | 604 | 605 |
| 管理番号 | 支払金額 | 申請人情報 | 有効期限 | 署名 |

【図7】

支払証明書管理DBの内容

| | | | | | |
|------|------|-------|------|------|------|
| 701 | 702 | 703 | 704 | 705 | 706 |
| 管理番号 | 支払金額 | 申請人情報 | 有効期限 | 署名情報 | 使用状況 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

【図8】

チケットの内容

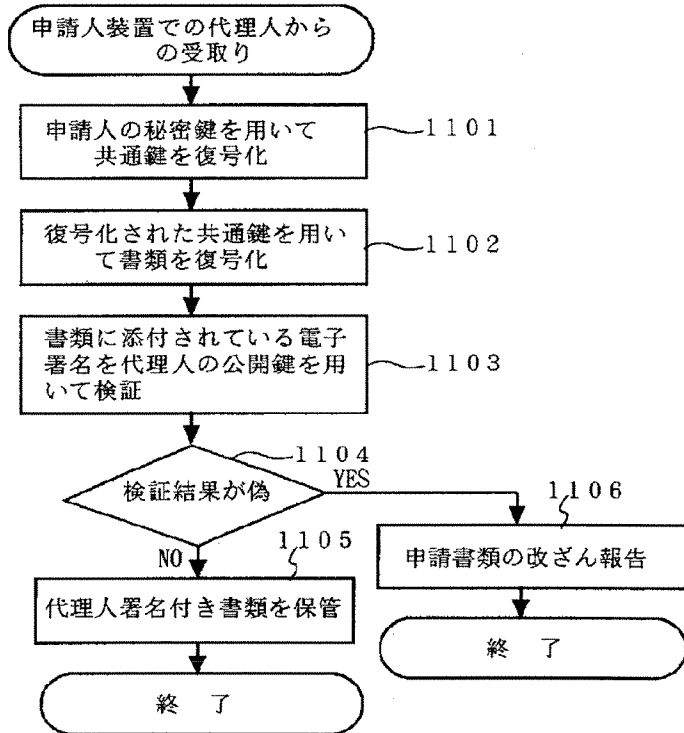
| | | | |
|------|-------|------|-----|
| 801 | 802 | 803 | 804 |
| 受付番号 | 送信者情報 | 有効期限 | 署名 |

【図9】

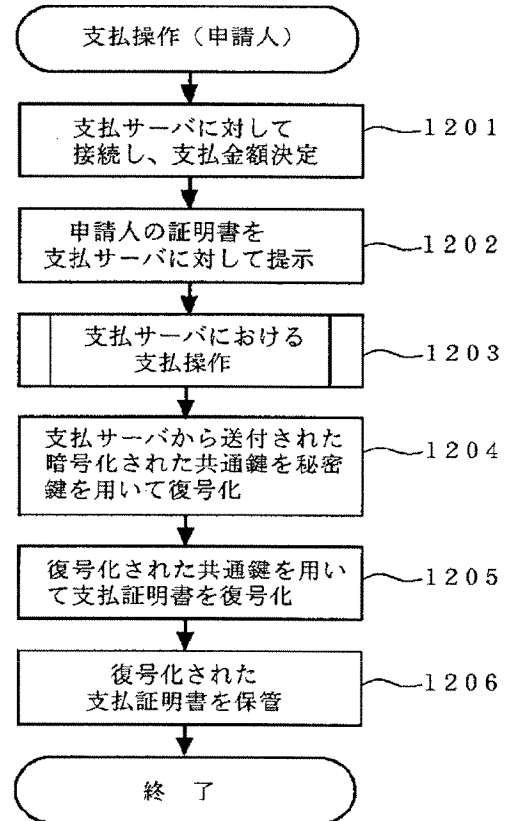
受付管理DBの内容

| 901 | 902 | 903 | 904 | 905 | 906 | 907 |
|------|-------|------|------------------|------------|--------------|-------|
| 受付番号 | 送信者情報 | 有効期限 | メッセージ タイムスタンプ | 送信者 証明書 | チケット管理 情報 | 書類の内容 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

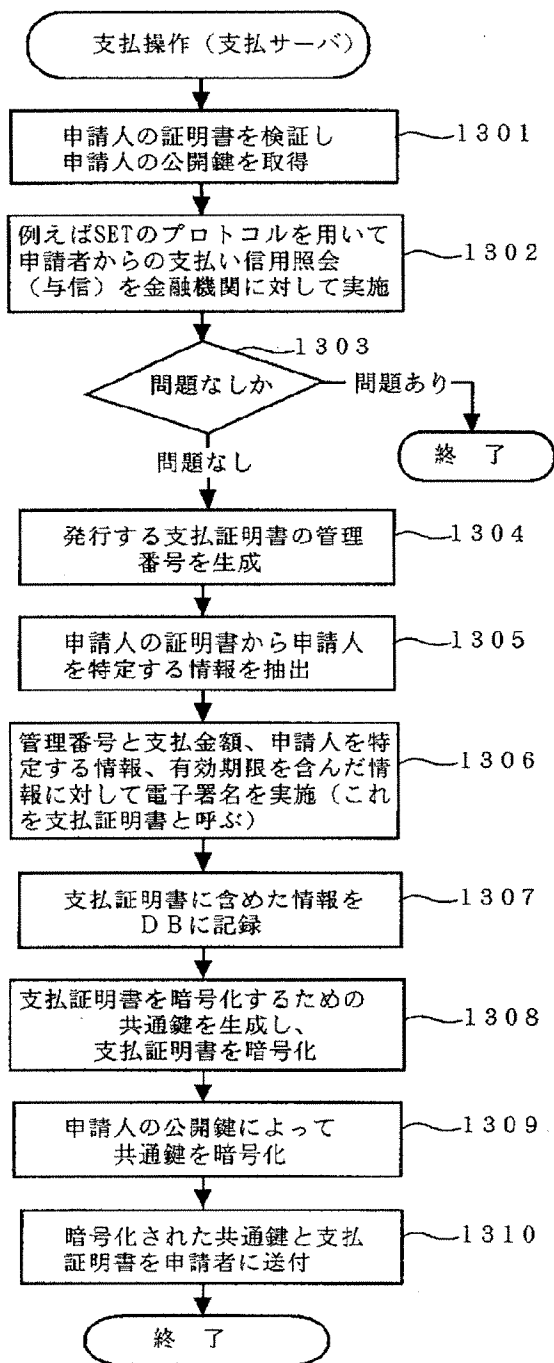
【図11】



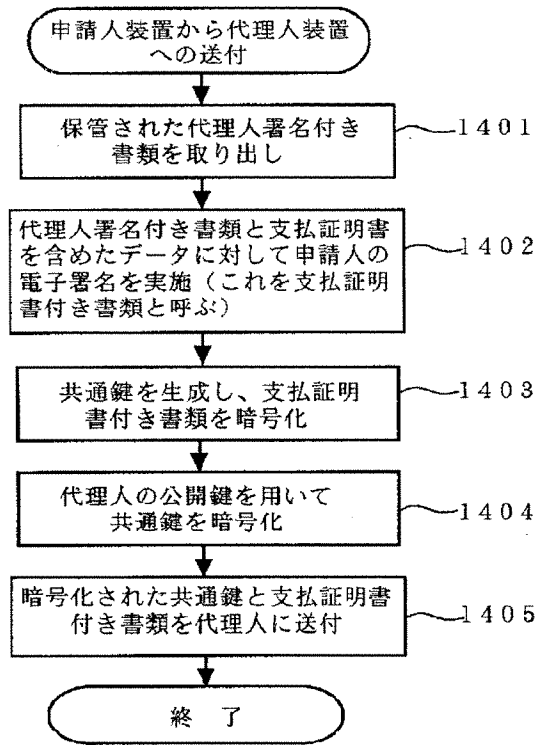
【図12】



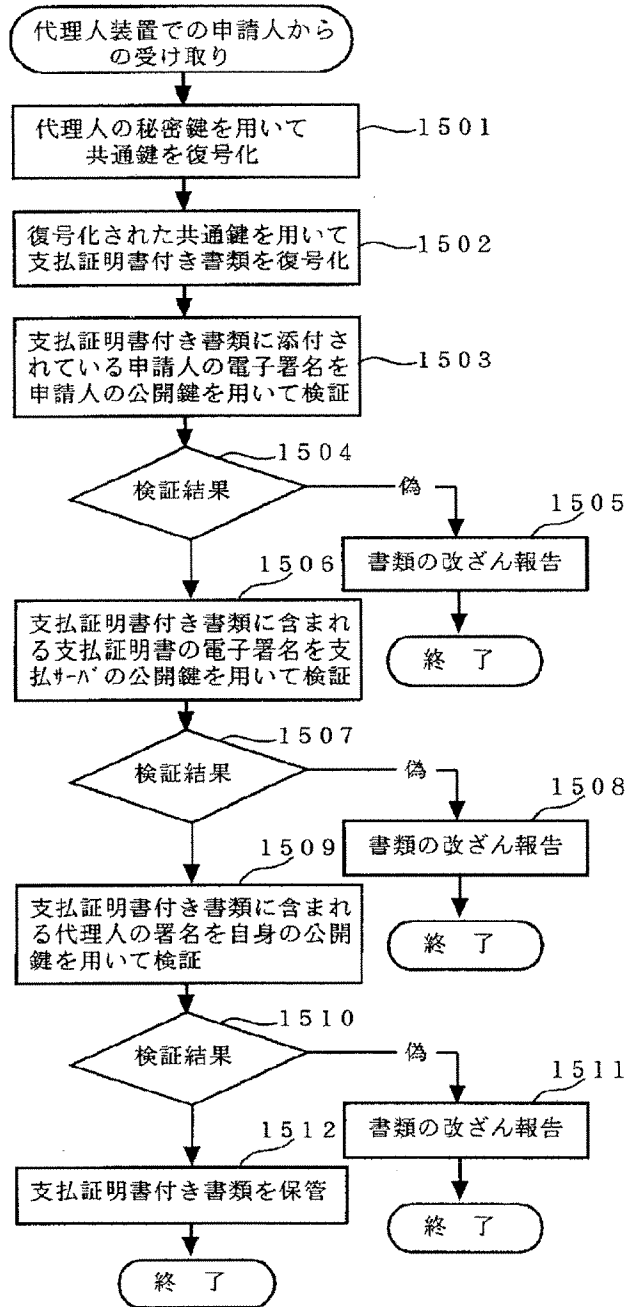
【図13】



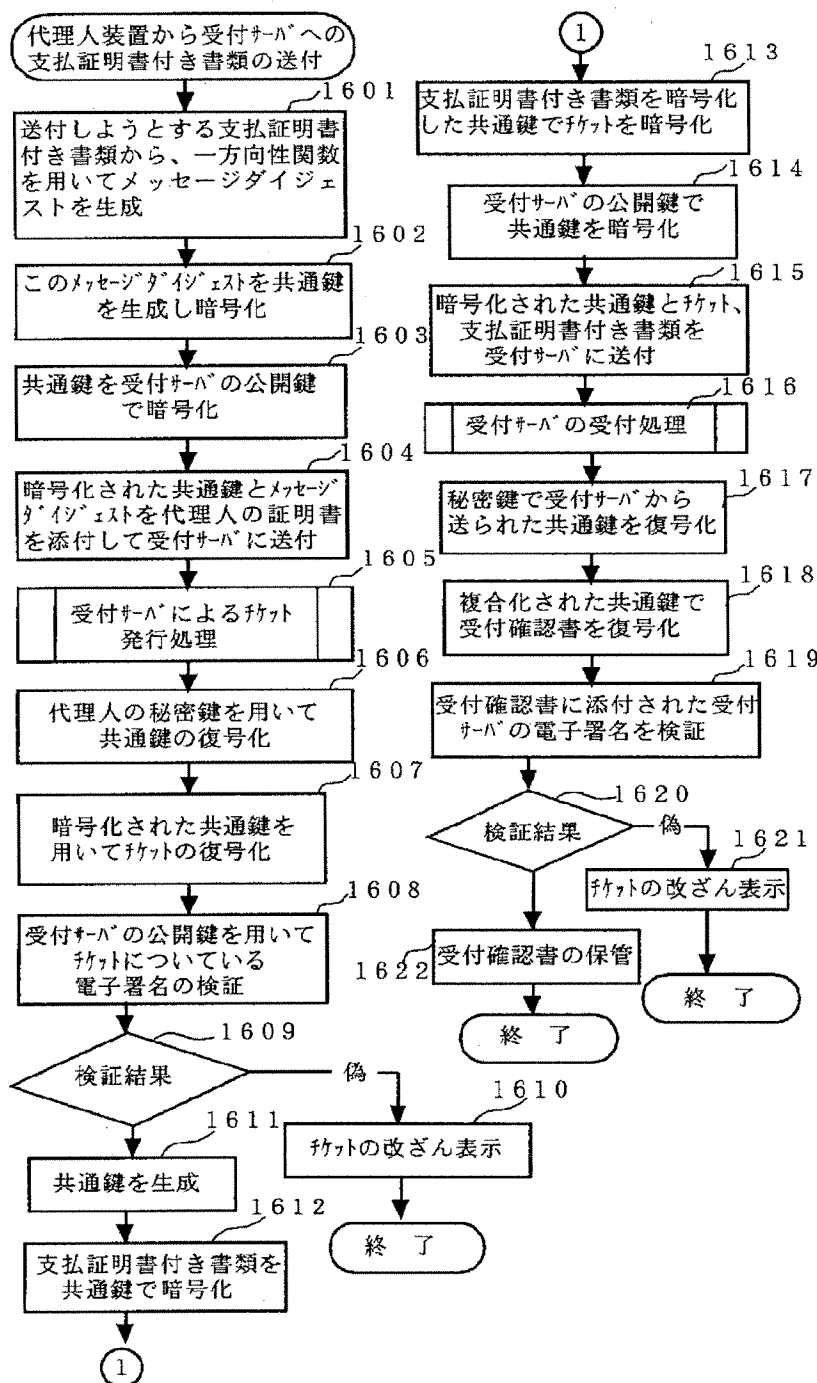
【図14】



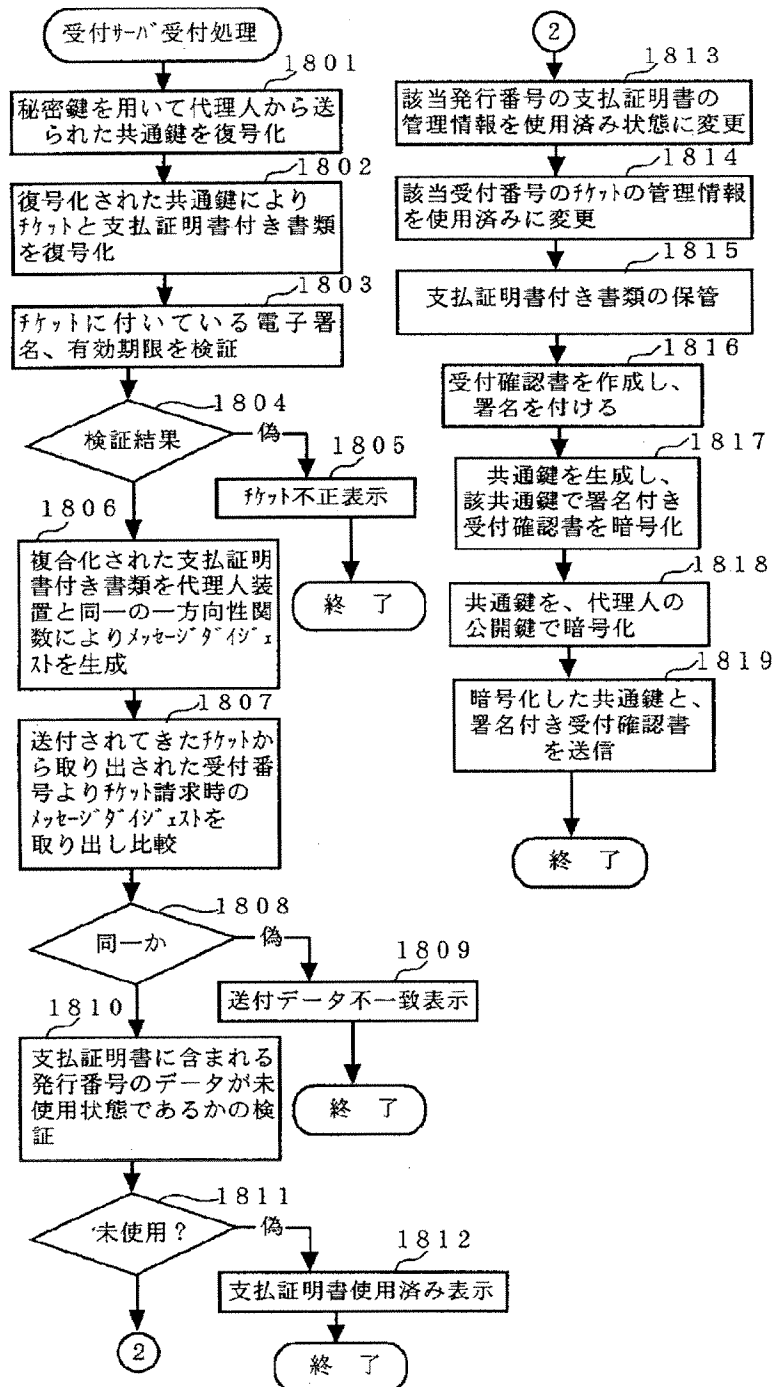
【図15】



【図16】



【図18】



【公報種別】特許法第17条の2の規定による補正の掲載
 【部門区分】第6部門第3区分
 【発行日】平成13年2月23日(2001.2.23)

【公開番号】特開平11-175607
 【公開日】平成11年7月2日(1999.7.2)
 【年通号数】公開特許公報11-1757
 【出願番号】特願平9-352243
 【国際特許分類第7版】

G06F 17/60

【F1】

G06F 15/21 Z

【手続補正書】

【提出日】平成11年9月10日(1999.9.10)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】データ送付方法、装置及びシステム並びにその方法を格納した記録媒体

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】ネットワークで接続された第1、第2、第3の計算機を有し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機から前記第3の計算機に対して認証を依頼するステップと、前記第1の計算機からの認証依頼に応じて、前記第3の計算機で認証を行い、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第1の計算機に送付するステップと、前記第3の計算機からの証明書データを受けて、前記第1の計算機で送付する電子化データに前記証明書データを付して証明書付きデータとし、前記第2の計算機に送付するステップと、前記第1の計算機からの証明書付きデータを受けて、前記第2の計算機で証明書データが未使用のものであることを確認し、当該証明書付きデータを保管するステップとを備えたことを特徴とするデータ送付方法。

【請求項2】第1、第2、第3の計算機が接続されたネットワークを利用し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機から前記第3の計算機に対して認証を依頼するステップと、前記第3の計算機から認証結

果を受け、前記第2の計算機に送付する電子化データに前記認証結果を付した認証付きデータとし、前記第2の計算機に送付するステップとを備えたことを特徴とするデータ送付方法。

【請求項3】ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とするデータ送付方法。

【請求項4】ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記圧縮データを受信後、前記第1の計算機に受信を示す受信済みデータを送付するステップと、前記第1の計算機で、前記受信済みデータを受信後、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とするデータ送付方法。

【請求項5】ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付方法であって、前記電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記他の計算機に送付するステップと、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データを前記他の計算機に送付するステップとを備えたことを特徴とするデータ送付方法。

【請求項6】ネットワークで接続された第1、第2、第3の計算機を有し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付システムであって、前記第1の計算機は、前記第3の計算機に対して認

証を依頼する手段を備え、前記第3の計算機は、前記第1の計算機からの認証依頼に応じて認証を行う手段と、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第1の計算機に送付する手段とを備え、前記第1の計算機は、前記第3の計算機からの証明書データを受けて、電子化データに前記証明書データを付して証明書付きデータとし、前記第2の計算機に送付する手段を備え、前記第2の計算機は、前記第1の計算機からの証明書付きデータを受けて、証明書データが未使用のものであることを確認し、当該証明書付きデータを保管する手段を備えたことを特徴とするデータ送付システム。

【請求項7】第1、第2の計算機が接続されたネットワークを利用して、前記第1の計算機へ電子化データを送付するデータ送付装置であって、前記第2の計算機に対して認証を依頼する手段と、前記第2の計算機から認証結果を受け取る手段と、前記第1の計算機に送付する電子化データに前記認証結果を付した認証付きデータを作成する手段と、当該認証付きデータを前記第1の計算機に送付する手段とを備えたことを特徴とするデータ送付装置。

【請求項8】ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付システムであって、前記第1の計算機は、電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記第2の計算機に送付する手段と、前記電子化データを前記第2の計算機に送付する手段とを備え、前記第2の計算機は、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較する手段とを備えたことを特徴とするデータ送付システム。

【請求項9】ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付装置であって、前記電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記他の計算機に送付する手段と、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データの前記他の計算機への送付を実行する手段とを備えたことを特徴とするデータ送付装置。

【請求項10】第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法を実現するプログラムを格納した記録媒体であって、前記データ送付方法は以下を含む：前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップ。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正内容】

【0001】

【発明の属する技術分野】本発明は、電子データで各種の書類を送付・受付し、該書類の送付・受付に伴う料金の支払いやその支払い受付を行なうデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体に関する。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正内容】

【0009】本発明は、上述の従来形における問題点を鑑み、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者が異なる場合でも適正に書類提出とその料金支払いを行なうことができるデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体を提供することを目的とする。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】また、本発明は、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えたデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体を提供することを目的とする。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】

【課題を解決するための手段】上記目的を達成するため、本発明は、ネットワークで接続された第1、第2、第3の計算機を有し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機から前記第3の計算機に対して認証を依頼するステップと、前記第1の計算機からの認証依頼に応じて、前記第3の計算機で認証を行い、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第1の計算機に送付するステップと、前記第3の計算機からの証明書データを受けて、前記第1の計算機で送付する電子化データに前記証明書データを付

して証明書付きデータとし、前記第2の計算機に送付するステップと、前記第1の計算機からの証明書付きデータを受けて、前記第2の計算機で証明書データが未使用のものであることを確認し、当該証明書付きデータを保管するステップとを備えたことを特徴とする。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正内容】

【0012】また本発明は、第1、第2、第3の計算機が接続されたネットワークを利用し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機から前記第3の計算機に対して認証を依頼するステップと、前記第3の計算機から認証結果を受け、前記第2の計算機に送付する電子化データに前記認証結果を付した認証付きデータとし、前記第2の計算機に送付するステップとを備えたことを特徴とする。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正内容】

【0013】また本発明は、ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とする。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正内容】

【0014】また本発明は、ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法であって、前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記圧縮データを受信後、前記第1の計算機に受信を示す受信済みデータを送付するステップと、前記第1の計算機で、前記受信済みデータを受信後、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とする。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正内容】

【0015】また本発明は、ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付方法であって、前記電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記他の計算機に送付するステップと、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データを前記他の計算機に送付するステップとを備えたことを特徴とする。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正内容】

【0016】また本発明は、ネットワークで接続された第1、第2、第3の計算機を有し、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付システムであって、前記第1の計算機は、前記第3の計算機に対して認証を依頼する手段を備え、前記第3の計算機は、前記第1の計算機からの認証依頼に応じて認証を行う手段と、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第1の計算機に送付する手段とを備え、前記第1の計算機は、前記第3の計算機からの証明書データを受けて、電子化データに前記証明書データを付して証明書付きデータとし、前記第2の計算機に送付する手段を備え、前記第2の計算機は、前記第1の計算機からの証明書付きデータを受けて、証明書データが未使用のものであることを確認し、当該証明書付きデータを保管する手段を備えたことを特徴とする。また本発明は、第1、第2の計算機が接続されたネットワークを利用して、前記第1の計算機へ電子化データを送付するデータ送付装置であって、前記第2の計算機に対して認証を依頼する手段と、前記第2の計算機から認証結果を受けとる手段と、前記第1の計算機に送付する電子化データに前記認証結果を付した認証付きデータを作成する手段と、当該認証付きデータを前記第1の計算機に送付する手段とを備えたことを特徴とする。また本発明は、ネットワーク経由で、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付システムであって、前記第1の計算機は、電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記第2の計算機に送付する手段と、前記電子化データを前記第2の計算機に送付する手段とを備え、前記第2の計算機は、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較する手段とを備えたことを特徴とする。また本発明は、ネットワーク経由で、他の計算機に対して電子化データを送付するデータ

送付装置であって、前記電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記他の計算機に送付する手段と、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データの前記他の計算機への送付を実行する手段とを備えたことを特徴とする。また本発明は、第1の計算機から第2の計算機に対して電子化データを送付するデータ送付方法を実現するプログラムを格納した記録媒体であって、前記

データ送付方法は以下を含むことを特徴とする：前記第1の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第2の計算機に送付するステップと、前記電子化データを前記第2の計算機に送付するステップと、前記第2の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップ。